

REMARKS

The Applicant and the undersigned thank Examiner Nalven for his careful review of this application. Claims 41-70 have been rejected by the Examiner. Upon entry of this amendment, Claims 56-60 and 66-70 have been cancelled, and Claims 41-55, and 61-65 remain pending in this application. The three remaining independent claims are Claims 41, 47 and 61.

Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Summary of Telephonic Interview of November 17, 2004

The Applicant and the undersigned thank the Examiner for his time and consideration given during the telephonic interview of November 17, 2004. During this telephonic interview, a proposed amendment to the claims was discussed. The Applicant provided the proposed amendment to the claims in advance of the interview.

Examiner Nalven provided his thoughts on the proposed changes to the claims. The Examiner stated that he did not believe that the prior art of record (U.S. Pat. No. 6,530,024 issued in the name of Paul E. Proctor, hereinafter the "Proctor" reference); EPO Patent No. EP 0 793 170 issued in the name of Graham Hamilton (hereinafter the "Hamilton" reference); and U.S. Pat. No. 5,991,881 issued in the name of Conklin et al. (hereinafter the "Conklin" reference) provides any teaching of (1) a remote monitoring center which operates at a location other than a site of any one of the customers (as recited only in independent Claim 41) and (2) a network intrusion prevention device operative to make the determination that a communication represents a security risk independently after being configured and without control from the remote monitoring center (as recited in each independent claim).

Examiner Nalven also requested that the Applicant indicate what parts of the originally filed patent application provide support for the two amended claim elements discussed above. The Applicant's representative indicated that the parts of the application providing support for the amended claim elements would be indicated in the next response. The Applicant notes that support for these two amended claim elements are discussed below.

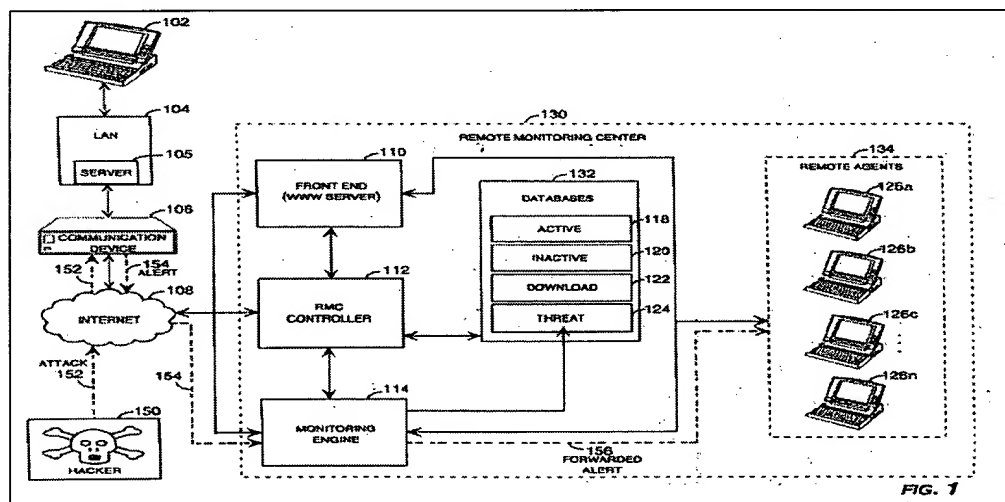
The Applicant and the undersigned request the Examiner to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date

next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202. Consideration and approval of this interview summary record are respectfully requested.

Support for Amended Claim Elements

The Examiner requested that the Applicant indicate the parts of the originally filed patent application that describe (1) a remote monitoring center which operates at a location other than a site of any one of the customers (as recited only in independent Claim 41) and (2) a network intrusion prevention device operative to make the determination that a communication represents a security risk independently after being configured and without control from the remote monitoring center (as recited in each independent claim).

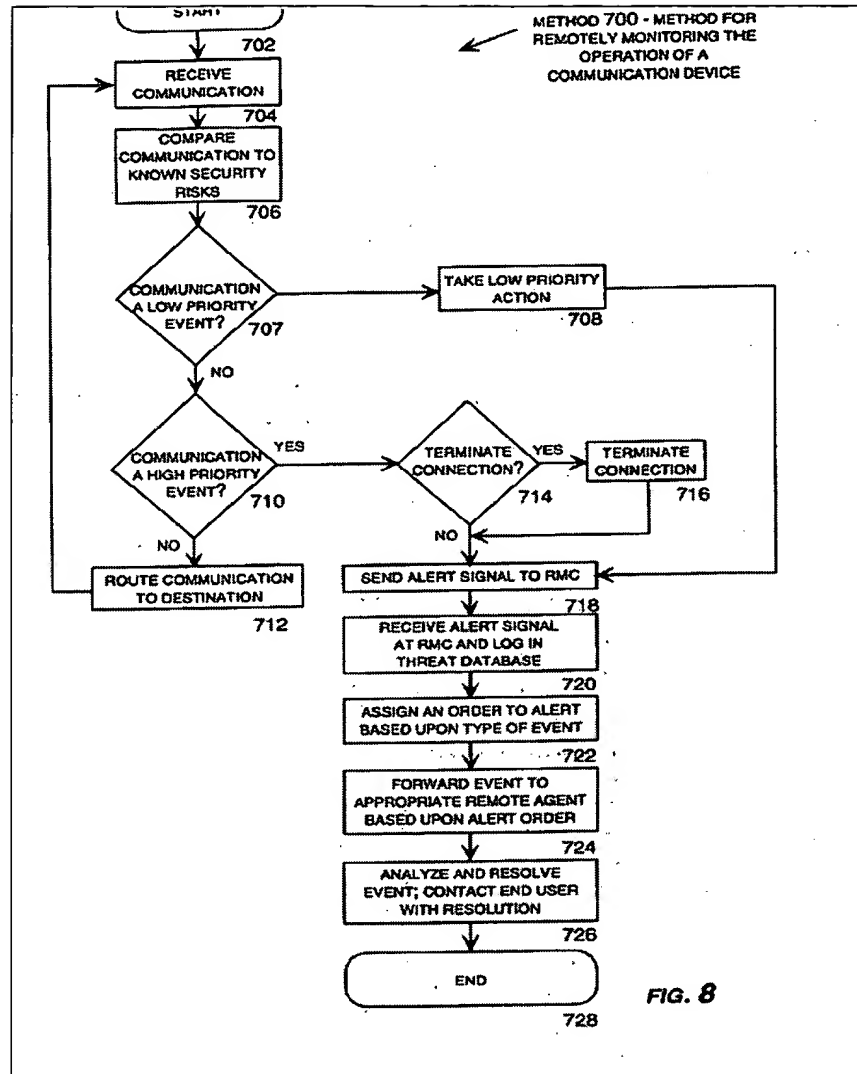
Regarding claim element (1) that describes a remote monitoring center which operates at a location other than a site of any one of the customers (as recited only in independent Claim 41) of the amendment, Figure 1 of the originally filed application illustrates a remote monitoring center 130 in a different location than that of a network intrusion prevention device 106. See Figure 1 of the originally filed application reproduced below.



The remote monitoring center 130 communicates with the network intrusion prevention device 106 through the internet 108. Page 3, lines 15-21 of the originally filed application describes a system for remotely configuring and monitoring a communication device 106 (network intrusion prevention device as now claimed). The network intrusion prevention device 106 can be configured for operation from a remote location through the internet 108. Page 16, lines 1-28 describe how the network intrusion prevention device 106 can be activated by a customer who accesses a web page supported by the remote monitoring center 130. The customer can provide a

unique identification number (UIN) that corresponds to the customer's network intrusion prevention device 106 and the customer's billing information that includes, but is not limited to, a customer's name, address, telephone number, credit card number, e-mail address, password, and other like information.

Regarding claim element (2) of the amendment, support for the network intrusion prevention device operating to make the determination that a communication represents a security risk independently and without control from the remote monitoring device after configuration of the network intrusion prevention device exists in the originally filed patent application on page 14, lines 11-26. This portion of the application explains how the network intrusion prevention device 106 utilizes a stored collection of attack signatures to monitor computer communications to determine if any of those communications match one of the prestored signatures. Upon detecting an attack, the network intrusion prevention device may transmit an alert signal via the RMC communication module 165 to indicate to the remote monitoring center 130 that an intrusion has taken place. The network intrusion prevention device 106 may also take other appropriate action such as terminating a communication. See originally filed application, page 28, lines 21-26 that describe step 714 of Figure 8 for terminating a communication.



In summary, the Applicant submits that support for the two amended claim elements discussed above is present in the originally filed application. Reconsideration and an early notice of allowance of this patent application are respectfully requested.

Rejections under 35 U.S.C. § 103

The Examiner rejected Claims 41-43, 45, 47-52, 54, 56-58, 61-62, and 64-70 under 35 U.S.C. § 103(a) as being obvious over the Proctor reference in view of the Hamilton and Conklin references. The Examiner rejected Claims 44, 53, and 59 under 35 U.S.C. § 103(a) as being obvious over the Proctor, Hamilton, Conklin references in view of U.S. Pat. No. 6,012,100 issued in the name of Frailong et al. (hereinafter, the "Frailong" reference).

The Examiner rejected Claims 46, 55, and 60 under 35 U.S.C. § 103(a) as being obvious over the Proctor, Hamilton, Conklin references in view of U.S. Pat. No. 6,324,692 issued in the name of Fiske (hereinafter, the “Fiske” reference) and U.S. Pat. No. 6,301,668 issued in the name of Gleichauf (hereinafter, the “Gleichauf” reference). The Examiner rejected Claim 63 under 35 U.S.C. § 103(a) as being obvious over the Proctor, Hamilton, Conklin references in view of U.S. Pat. No. 6,289,201 issued in the name of Weber et al. (hereinafter, the “Weber” reference)/

The Applicant respectfully offers remarks to traverse these rejections. The Applicant will address each independent claim separately as the Applicant believes that each independent claim is separately patentable over the prior art of record.

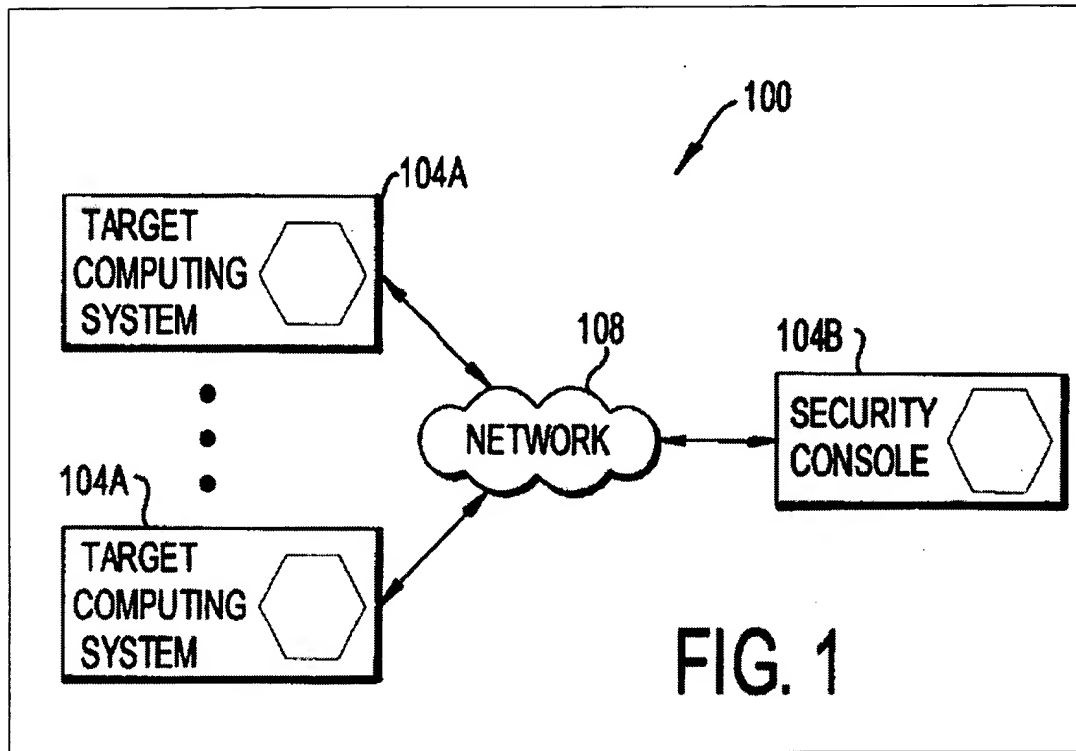
Independent Claim 41

The rejection of Claim 41 is respectfully traversed. It is respectfully submitted that the Proctor, Hamilton, Conklin, Frailong, Fiske, Gleichauf, and Weber references fail to describe, teach, or suggest the combination of: (1) receiving at the remote monitoring center a first transmission comprising a first identification number and a network address associated with one of a plurality of network intrusion prevention devices monitored by the remote monitoring center which operates at a location other than a site of any one of the customers, each network intrusion prevention device positioned in-line with and between a computer network controlled by one of the customers and a distributed computer network that is not controlled by the customers, (2) each network intrusion prevention device operative to block a communication from passing to the corresponding computer network via the distributed computer network by terminating the communication based on a determination that the communication represents a security risk to at least one of the computers coupled to the computer network, (3) each network intrusion prevention device operative to make the determination that the communication represents a security risk independently after being configured and without control from the remote monitoring center, each network intrusion prevention device comprising a firewall, an intrusion detector, and a remote monitoring controller communication module, wherein the remote monitoring controller communication module is operatively coupled to the remote monitoring center; (4) storing the identification number and network address for the network intrusion prevention device in a database at the remote monitoring center; (5) receiving at the remote monitoring center a second identification number during a second transmission from the network

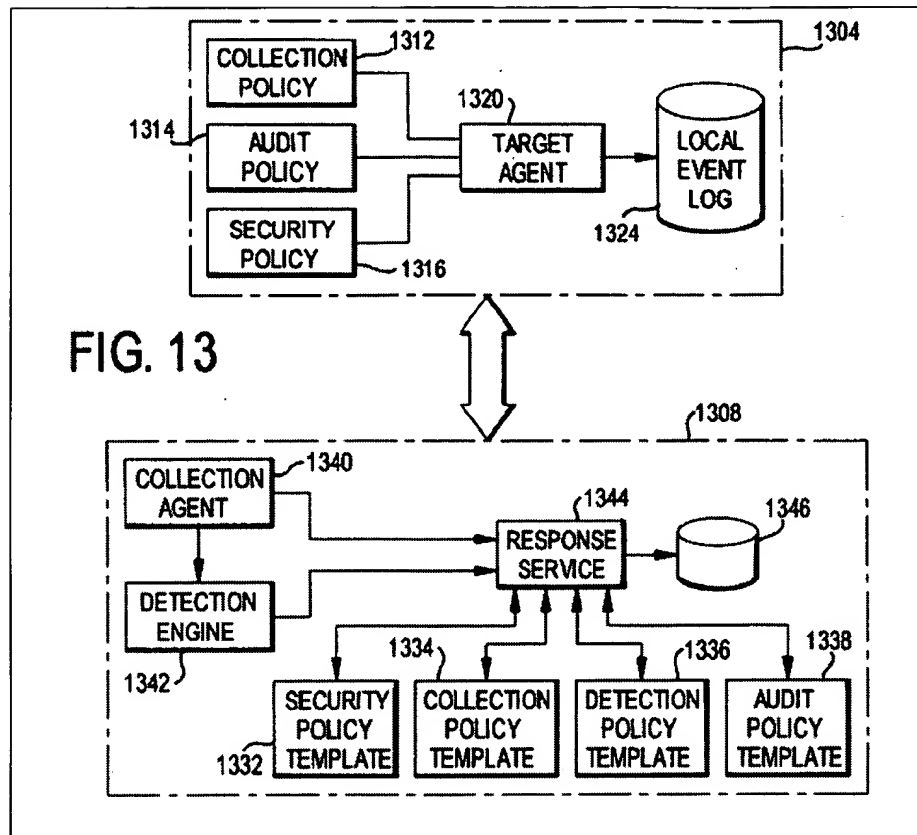
intrusion prevention communication device; (6) comparing the second identification number with the first identification number at the remote monitoring center and, in response to a match between the first identification number and second identification number, identifying a plurality of security policy options that are selectable by the network intrusion prevention device; (7) generating a configuration file with the remote monitoring center in response to selection of at least one of the security policy options by the network intrusion prevention device, the configuration file governing the intrusion protection operation for the network intrusion prevention communication device; (8) transmitting the configuration file from the remote monitoring center to configure the network intrusion prevention device; (9) monitoring the network intrusion prevention device by the remote monitoring center for issuance of an alert signal issued by the network intrusion prevention communication device in response to a determination that the communication represents a security risk to at least one of the computers coupled to the computer network; (10) receiving the alert signal at the remote monitoring center; and (11) assigning the alert signal an order and taking responsive action at the remote monitoring center based upon the assigned order, as recited in amended independent Claim 41.

The Proctor Reference

The Proctor reference describes a host-based security policy system that is opposite to the Applicant's network based intrusion prevention device. In the host-based security policy system of the Proctor reference, computers 104A of Figure 1 in a network 108 run audit modules 1304 illustrated in Figure 13. See Figure 1 and Figure 13 of the Proctor reference listed below.



The audit modules 1304 monitor information traffic from the network 108 and pass this information to a security console 104B that runs security procedure module 1308. The audit module 1304 can prevent information from entering an individual computer 104A based on procedures it receives from the security module 108 running the security console 104B. The security console 104B and individual computers are in constant communication so that the security console 104B that includes a response service 1344 can determine what action to take when a security threat is detected. See the Proctor reference, Figure 13, and column 14, lines 11-55, and especially lines 46-55.



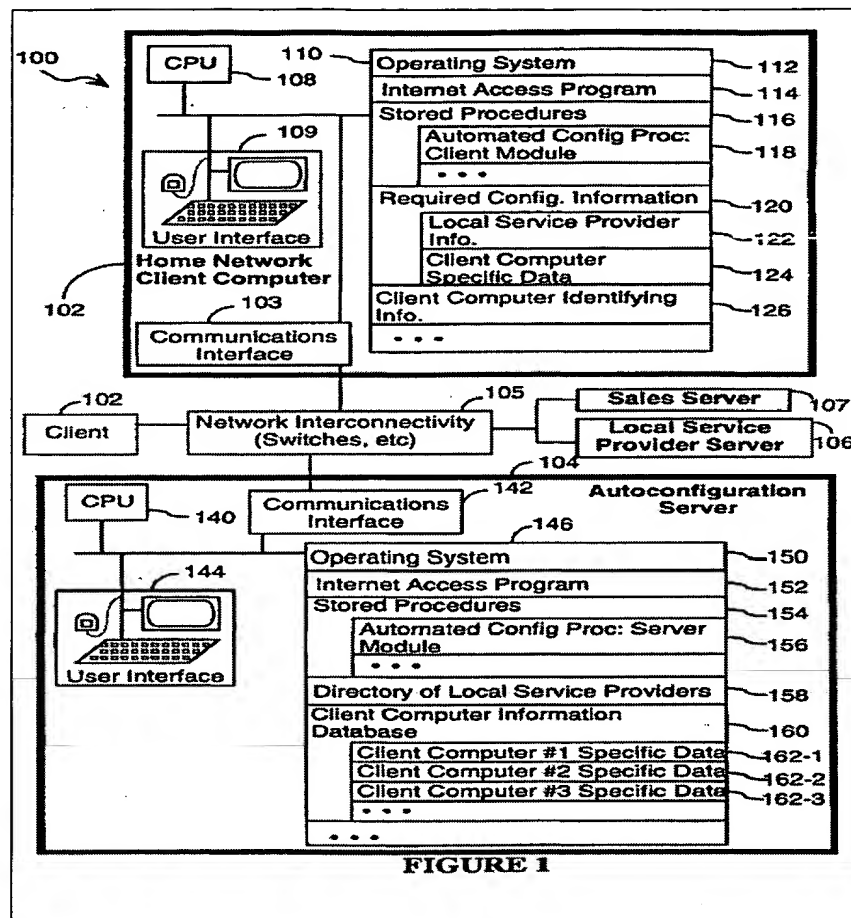
Therefore, the Proctor reference describes a host-based security policy system that is directly opposite to a network intrusion prevention device that is operative for making determinations that the communication represents a security risk independently after being configured and without control from the remote monitoring center, as recited in amended independent Claim 41. The Proctor reference also does not describe network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

The Hamilton Reference

The Examiner admits that the Proctor reference also fails to provide any teaching of sending, storing, and comparing identification numbers and subsequent configuration messages. To make up for these deficiencies, the Examiner relies upon the Hamilton reference.

The Hamilton reference describes a distributed computer system 100 with several home network client computers 102 and at least one remotely located autoconfiguration server 104 as illustrated in Figure 1 listed below. Each home network client computer 102 is connected to the autoconfiguration server via a communications network 105 such as the Internet. The home

network client computers 102 are generally desktop computers. See paragraph [0020] on page 4 of the Hamilton reference.



The autoconfiguration server 104 of the Hamilton reference is designed to provide client computers 102 with configuration information necessary for the client computers 102 to access a local internet service provider 106. To receive the configuration information from the server 104, each client computer 102 can send a request that includes a telephone number or serial number uniquely associated with the home network client computer 102 or both. See paragraph [0011] of Pages 2 and 3 of the Hamilton reference.

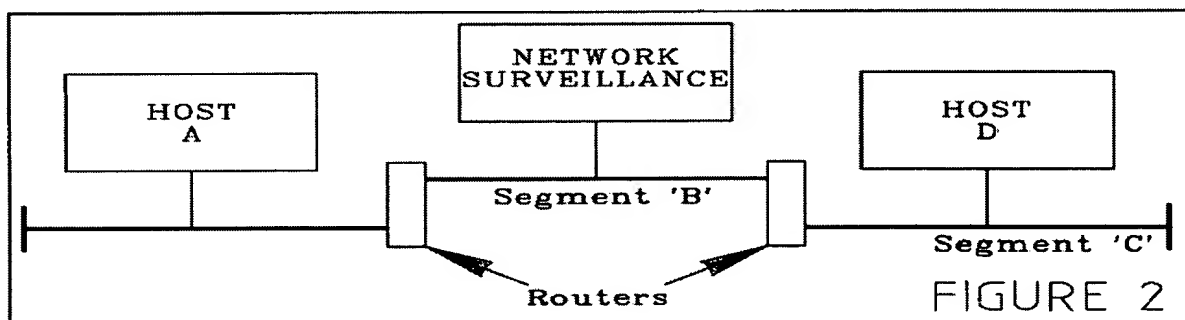
The Hamilton reference does not relate in any way to computer network security or network intrusion prevention devices. It logically follows that the Hamilton reference does not provide any teaching of a network intrusion prevention device that is operative for making determinations that the communication represents a security risk independently after being configured and without control from the remote monitoring center, as recited in amended independent Claim 41. The Hamilton reference, like the Proctor reference, also does not describe

network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

The Conklin Reference

The Examiner admits that the Proctor reference also fails to describe each network intrusion prevention device positioned in-line with a computer network. To make up for this deficiency, the Examiner relies upon the Conklin reference.

The Conklin reference describes systematic monitoring, intrusion identification, notification, and tracking of unauthorized activities, such as methods or systems used by “hackers” to intrude computer networks. The Conklin reference teaches a star configuration of two Ethernet network segments ‘B’ and ‘C’ and a terminal network connection leading to a network surveillance device for a computer network as illustrated in Figure 2. The system of the Conklin reference broadcasts communications between any two computers on an Ethernet segment that is monitored by an out-of-line surveillance device. See Conklin reference, column 2, lines 58-66.

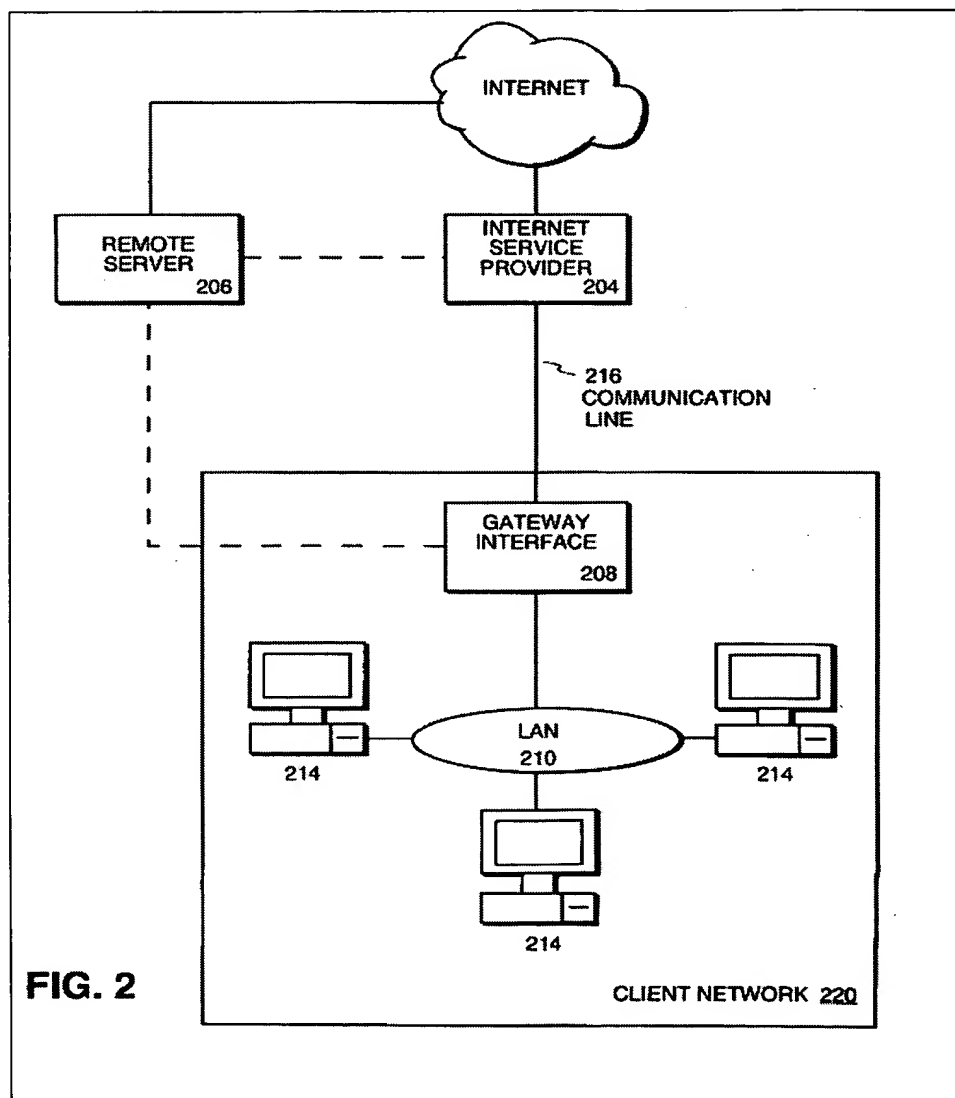


The Conklin reference does not describe any intrusion prevention. Instead, the Conklin reference is designed for intrusion detection or surveillance. It follows that the Conklin reference does not provide any teaching of a network intrusion prevention device that is operative for making determinations that the communication represents a security risk independently after being configured and without control from a remote monitoring center, as recited in amended independent Claim 41. The Conklin reference, like the Proctor reference, also does not describe network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

The Frailong Reference

The Examiner admits that the Proctor reference does not teach diagnostic variables being used to ensure proper operation of a communication device. To make up for these deficiencies, the Examiner relies upon the Frailong reference.

The Frailong reference describes a network interface device 208 that is provided to connect a client computer network 220 to an external network 204. The network device 208 is configured for the client system by automated procedures and protocols from a remote server 206. The remote server 206 provides and maintains the client information in a secure database. See Frailong reference, column 5, lines 1-35.



The Frailong reference does not relate in any way to computer network security or network intrusion prevention devices. It logically follows that the Frailong reference does not provide any

teaching of a network intrusion prevention device that is operative for making determinations that the communication represents a security risk independently after being configured and without control from a remote monitoring center, as recited in amended independent Claim 41. The Frailong reference, like the Proctor reference, also does not describe network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

The Fiske Reference

The Examiner admits that the Proctor reference fails to provide any teaching of a configuration complete signal. To make up for this deficiency, the Examiner relies upon the Fiske reference.

The Fiske reference describes a system for upgrading a computer program. An upgraded version of a program is received into a processor and a backup of the program is created in memory associated with the processor. The upgraded version of the program is then installed and the processor is rebooted. See Fiske reference, column 1, lines 53-65.

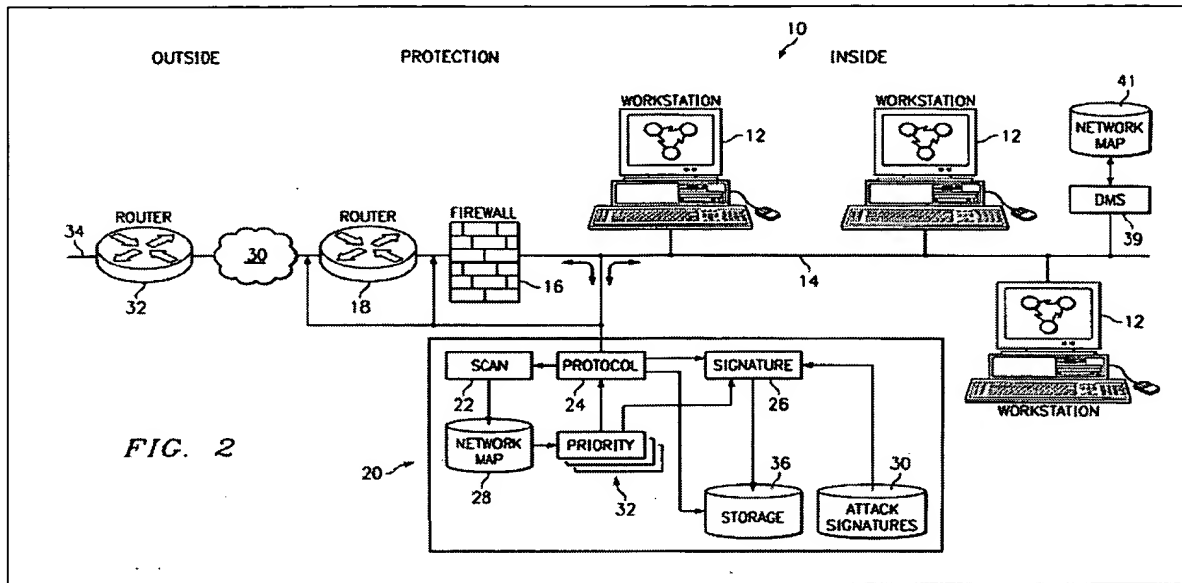
The Fiske reference does not relate in any way to computer network security or network intrusion prevention devices. It logically follows that the Fiske reference does not provide any teaching of a network intrusion prevention device that is operative for making determinations that the communication represents a security risk independently after being configured and without control from a remote monitoring center, as recited in amended independent Claim 41. The Fiske reference, like the Proctor reference, also does not describe network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

The Gleichauf Reference

The Examiner admits that the Proctor reference fails to provide any teaching of performing a vulnerability analysis on a communication device. To make up for this deficiency, the Examiner relies upon the Gleichauf reference.

The Gleichauf reference describes a network security system 20 that sends requests upon a network backbone 14 through a scan engine 22 and analyzes responses to such requests to discover network information of internal network 10. Scan engine 22 can ping devices, use port

scans, and other methods, and/or rules-driven, multi-phase network vulnerability assessment process to discover network information such as devices, operating systems, and services on the internal network 10. See Figure 2 of the Gleichauf reference reproduced below and see column 7, lines 41-43.



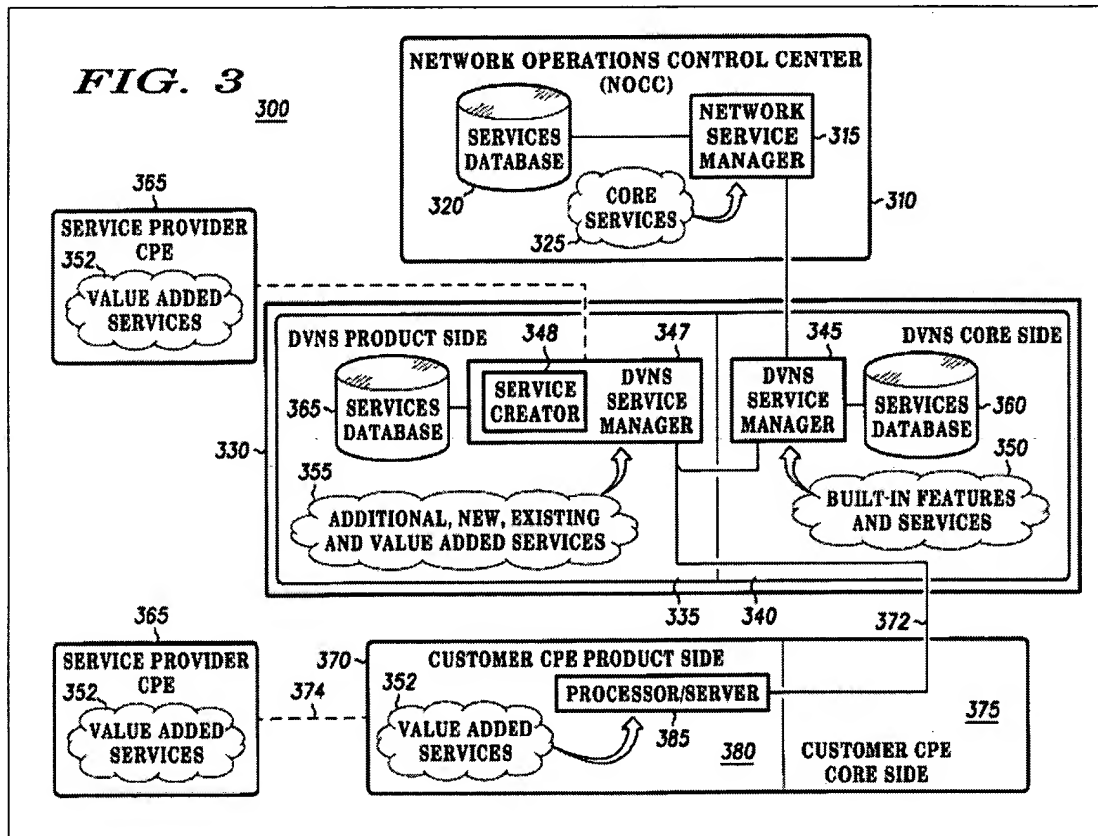
While it may be argued that the scan engine 22 of the network security system 20 of the Gleichauf reference is an intrusion detector, one of ordinary skill in the art recognizes that this system 20 does not include a firewall and remote communications module operatively coupled to a remote monitoring center. In fact, the Gleichauf reference expressly teaches away from a network intrusion prevention device that includes a firewall. The Gleichauf reference illustrates a firewall 16 that is completely separate from the network security system 20.

Meanwhile, amended independent Claim 41 describes network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

The Weber Reference

The Examiner admits that the Proctor reference fails to provide any teaching of agent personnel under control of a service provider while the communication devices are under control of entities subscribing to the network. To make up for this deficiency of the Proctor reference, the Examiner relies upon the Weber reference.

The Weber reference describes a multilayer service management in a satellite communication system. In the embodiment illustrated in Figure 3, the satellite communications system of the Weber reference includes a core service layer managed by NOCC 310, a DVNS services layer managed by DVNS 330, a value added services layer managed by DVNS 330 and provided by CPE layer 370. See Weber reference, column 5, lines 21-36 and Figure 3 reproduced below.



The Weber reference does not relate in any way to computer network security or network intrusion prevention devices. It logically follows that the Weber reference does not provide any teaching of a network intrusion prevention device that is operative for making determinations that the communication represents a security risk independently after being configured and without control from a remote monitoring center, as recited in amended independent Claim 41. The Weber reference, like the Proctor reference, also does not describe network intrusion prevention devices that include a firewall, an intrusion detector, and a remote monitoring controller communication module.

Summary for Analysis of Independent Claim 41 Rejection

In light of the differences between amended Claim 41 and the Proctor, Hamilton, Conklin, Frailong, Fiske, Gleichauf, and Weber references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 41. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 47

The rejection of Claim 47 is respectfully traversed. It is respectfully submitted that the Proctor, Hamilton, Conklin, Frailong, Fiske, Gleichauf, and Weber references fail to describe, teach, or suggest a network intrusion prevention device operative for: (1) presenting security policy options with the remote monitoring center, the security policy options selectable by each of the network intrusion prevention communication devices, (2) each network intrusion prevention communication device positioned in-line and between a computer network under control of one of a plurality of customers and a distributed computer network that is not under control of the customers; (3) generating a configuration file with the remote monitoring center in response to selection of the security policy options by each of the network intrusion prevention communication devices; (4) transmitting the configuration file from the remote monitoring center to configure the network intrusion prevention communication devices, each network intrusion prevention communication device operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to a corresponding one of the computer networks to determine whether the communication represents a security risk to the computer network in accordance with the configuration file, (5) each network intrusion prevention device operative to determine whether the communication represents a security risk independently after being configured and without control from the remote monitoring center, (6) the network intrusion prevention communication device further operative to issue an alert signal and to terminate the communication in response to a determination that the communication represents a security risk, (7) each network intrusion prevention device comprising a firewall, an intrusion detector, and a remote monitoring controller communication module, the remote monitoring controller communication module coupled to the remote monitoring center; (8) monitoring the network intrusion prevention communication devices with the remote monitoring

center to detect an issuance of the alert signal from one of the network intrusion prevention communication devices; (9) receiving the alert signal with the remote monitoring center; and (10) forwarding the alert signal to a remote agent associated with the service provider, wherein the alert signal provides an advisory of the security risk faced by the network intrusion prevention communication device that issued the alert signal, as recited in amended independent Claim 47.

Similar to the analysis of independent Claim 41, the Examiner's proposed combination of references fails to address that each network intrusion prevention device is operative to determine whether the communication represents a security risk independently after being configured and without control from the remote monitoring center. The proposed combination also fails to teach a network intrusion prevention communication device that comprises a firewall, an intrusion detector, and a remote monitoring controller communication module, the remote monitoring controller communication module coupled to the remote monitoring center; as recited in amended independent Claim 47.

In light of the differences between amended Claim 47 and the Proctor, Hamilton, Conklin, Frailong, Fiske, Gleichauf, and Weber references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 47. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 61

The rejection of Claim 61 is respectfully traversed. It is respectfully submitted that the Proctor, Hamilton, Conklin, Frailong, Fiske, Gleichauf, and Weber references fail to describe, teach, or suggest a system that includes: (1) a plurality of network intrusion prevention devices, each network intrusion prevention coupled in-line with and between one of the computer networks associated with a particular one of the entities and a distributed computer network that is not associated with any of the entities, (2) wherein each network intrusion prevention device is operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to the corresponding computer network to determine whether the communication represents a security risk to the computer network, and (3) wherein each network intrusion prevention device is further operative to block the communication from passage to the computer network by terminating the communication and to transmit an alert

signal via the distributed computer network in response to a determination by the network intrusion prevention device that the communication represents a security risk, (4) each network intrusion prevention device operative to make the determination that the communication represents a security risk independently after being configured and without control of the remote monitoring center, (5) each network intrusion prevention device comprising a firewall, an intrusion detector, and a (6) remote monitoring controller communication module, the remote monitoring controller communication module coupled to the remote monitoring center; and (7) a remote monitoring center operated on behalf of the entities by a service provider, the remote monitoring center coupled to the distributed computer network, remotely located from each of the computer networks, and operative to monitor the security status of each one of the plurality of computer networks based upon status information transmitted by the network intrusion prevention communication devices for the computer networks, (8) the remote monitoring center responsive to receipt of the alert signal transmitted by any one of the network intrusion prevention communication devices to complete an analysis of the alert signal and to take a responsive action based on the analysis of the alert signal, as recited in amended independent Claim 61.

Similar to the analysis of independent Claim 41, the Examiner's proposed combination of references fails to address each network intrusion prevention device operative to make the determination that the communication represents a security risk independently after being configured and without control of the remote monitoring center. The references also fail to provide any teaching of a network intrusion prevention device comprising a firewall, an intrusion detector, as recited in amended independent Claim 61.

In light of the differences between amended Claim 61 and the Proctor, Hamilton, Conklin, Frailong, Fiske, Gleichauf, and Weber references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 61. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 42-46, 48-55, and 62-65

The Applicant respectfully submits that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited

references. The Applicant also respectfully submits that the recitations of these dependent claims are of patentable significance.

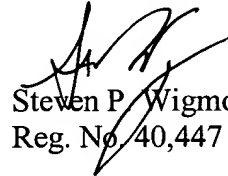
In view of the foregoing, the Applicant respectfully requests that the Examiner withdraw the pending rejections of dependent Claims 42-46, 48-55, and 62-65.

CONCLUSION

The foregoing is submitted as a full and complete response to the FINAL Office Action mailed on June 17, 2004. The Applicant and the undersigned thank Examiner Nalven for consideration of these remarks. The Applicant has amended the claims and has submitted remarks to traverse rejections of Claims 41-70. The Applicant respectfully submits that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, please contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,


Steven P. Wigmore
Reg. No. 40,447

KING & SPALDING, LLP
45th Floor, 191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 07609-105002